

SYSTEM, APPARATUS AND METHOD FOR REPLACING A CRYPTOGRAPHIC KEY

Publication number: JP2006513641 (T)

Publication date: 2006-04-20

Inventor(s):

Applicant(s):

Classification:

- international: H04L9/08; H04L9/30; H04L9/32; H04L9/06; H04L9/28; H04L9/32

- European: H04L9/30L; H04L9/32

Application number: JP20040566624T 20031230

Priority number(s): US20030438617P 20030107; WO2003US41538 20031230

Also published as:

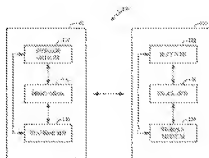
WO2004064312 (A1)
KR20050098864 (A)
EP2182671 (A1)
EP1582024 (A1)
EP1582024 (A4)

more >>

Abstract not available for JP 2006513641 (T)

Abstract of corresponding document: WO 2004064312 (A1)

Embodiments describe a method and/or system (200) whereby a secret key in a cryptographic system may be replaced without revealing the secret key. One embodiment comprises creating a first private key (210) and corresponding first public key (220) whereby a secret key in a cryptographic system may be replaced without revealing the secret key. A second private key associated with the first private key and a second public key corresponding to the second private key are also created (220). The second private key is output once (230) such that it can be re-created and the second public key is output when outputting the first public key (240). The first private key is used for authentication (260). The method further comprises re-creating the second private key; and using the second private key for authentication. Another embodiment comprises creating a private key and corresponding public key with associated system parameter (410); outputting the system parameter when outputting the public key (430); and using the private key for authentication (460). The method may further comprise creating a new private key using the previous key and the system parameter (470).



Data supplied from the **espacenet** database — Worldwide